

Web server

Bioinformatics Lab 2013

11 June 2013

Katharina Hembach

Overview

- set up apache
- php and CGI web pages
- phpldapadmin & LAM
- per-user web-accessible directories
- set up https
- create secure section

Installing Apache, simple web page

- `apt-get install apache2`
- default root folder is `/var/www`
- Edit `/var/www/index.html` to create a simple web page:

```
<html>
```

```
  <body><h1>Hello world! :)</h1>
```

```
    <p>This is a test web page that says "hello world!".</p>
```

```
  </body>
```

```
</html>
```

- Check if site is reachable: go to <http://kath.tbl/>

Set up php

- apt-get install libapache2-mod-php5
- Create /var/www/test.php:

```
<!DOCTYPE HTML>
<html>
  <head>
    <title>Text page</title>
  <body>
    <form action="" method="get">
      <input type="text" name="name"/>
      <input type="submit" value="Click me" />
    </form>
    <?php
      echo "Hello " . $_GET["name"] . "!";
      phpinfo();
    ?>
  </body>
</html>
```

- Go to <http://kath.tbl/test.php/>

Create CGI program (python)

```
#!/usr/bin/env python
import cgi
import os

print "Content-Type: text/html"
print

print """
    <!DOCTYPE HTML>
    <html>
        <head>
        <title>CGI text page</title>
        <body>
            <form action="" method="get">
                <input type="text" name="name"/>
                <input type="submit" value="Click me" />
            </form>

        """

form = cgi.FieldStorage()
name = form["name"].value

print "Hello " + name + "!"
```

CGI program (python)

```
#print environment variables
print "<font size=+1>Environment</font><br>"
for param in os.environ.keys():
    print "<b>%20s</b>: %s<br>" % (param, os.environ[param])

#print received parameters and their values
print "<p><font size=+1>The received parameters are:</font><br>"
for i in form:
    print "parameter: " + i + ", value: " + form[i].value + "<br>"
print "</p>"

print """
        </body>
    </html>
    """
```

- Make test.cgi executable: `chmod -x /var/www/test.cgi`

Allow CGI

- Edit the configuration file for apache2 (/etc/apache2/sites-available/default):
- Tell apache2
 - to permit the execution of CGI scripts: Options +ExecCGI
 - what files are CGI files: AddHandler cgi-script cgi py

```
<Directory /var/www/>
    Options Indexes FollowSymLinks MultiViews
    Options +ExecCGI
    AddHandler cgi-script cgi py
    AllowOverride None
    Order allow,deny
    allow from all
</Directory>
```

- Server restart with: **service apache2 restart**

Overview

- set up apache
- php and CGI web pages
- [phpldapadmin & LAM](#)
- per-user web-accessible directories
- Set up https
- Create secure section

Phpldapadmin



- apt-get install phpldapadmin
- web interface at <http://kath.tbl/phpldapadmin/>

Authenticate to server My LDAP Server

Warning: This web connection is unencrypted.

Login DN:




Password:



Anonymous ☐


LDAP-account-manager (LAM)

- apt-get install ldap-account-manager
- go to <http://kath.tbl/lam>
- LAM configurations: → Edit general settings:
 - Master password (first time “lam”)
 - New password




LDAP Account Manager

Please enter the master password to change the general preferences:



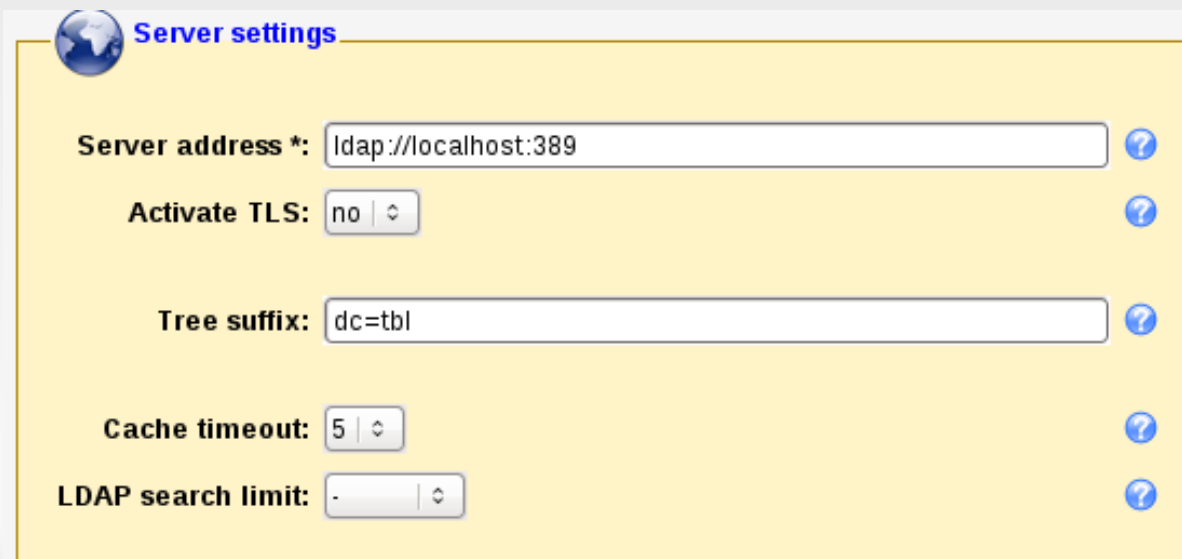
Change master password

New master password 

Reenter new master password

LAM configurations

- Edit server profiles:
 - Password “lam”
 - Tree suffix: dc=tbl
 - Login method: fixed list
 - Valid users: cn=admin,dc=tbl



Server settings

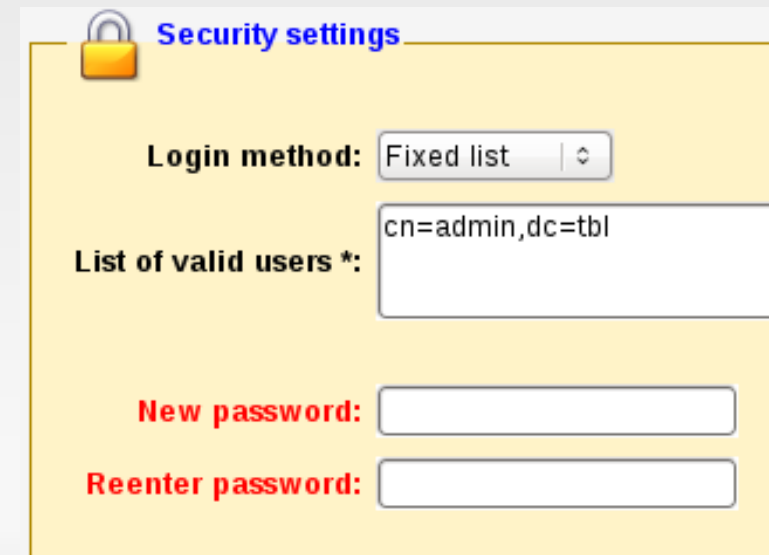
Server address *: ldap://localhost:389 ?

Activate TLS: no ?

Tree suffix: dc=tbl ?

Cache timeout: 5 ?

LDAP search limit: - ?



Security settings

Login method: Fixed list ?

List of valid users *: cn=admin,dc=tbl ?



New password: ?

Reenter password: ?

LAM configurations



- Account types:
 - Change ldap suffix for users and groups:
 - ou=People,dc=tbl
 - ou=group,dc=tbl

Active account types

 **Users:** User accounts (e.g. Unix, Samba and Kolab) 

LDAP suffix

List attributes

 **Groups:** Group accounts (e.g. Unix and Samba) 

LDAP suffix

List attributes

Overview

- set up apache
- php and CGI web pages
- phpldapadmin & LAM
- per-user web-accessible directories
- set https
- Create secure section

Per-user web-accessible directories with mod_userdir

- Module that allows user-specific directories to be accessed using the `http://kath.tbl/~user` syntax
- Enable module userdir: `a2enmod userdir`
- Restart apache to activate new configurations: `service apache2 restart`
- Per user content is loaded from `/home/user/public_html`
- Create `/home/kath/public_html/index.html`
- Check if `http://kath.tbl/~kath/` is reachable

Overview

- set up apache
- php and CGI web pages
- phpldapadmin & LAM
- per-user web-accessible directories
- set up https
- Create secure section

Set up https with tinyca2

- apt-get install tinyca
- start tinyca2 root

Create CA (as superuser)

Create a new CA

Name (for local storage): kath

Data for CA Certificate

Common Name (for the CA): kath

Country Name (2 letter code): de

Password (needed for signing): [masked]

Password (confirmation): [masked]

State or Province Name: Bayern

Locality Name (eg. city): Munich

Organization Name (eg. company): TUM

Organizational Unit Name (eg. section): Biolab

eMail Address: k.hembach@mytum.de

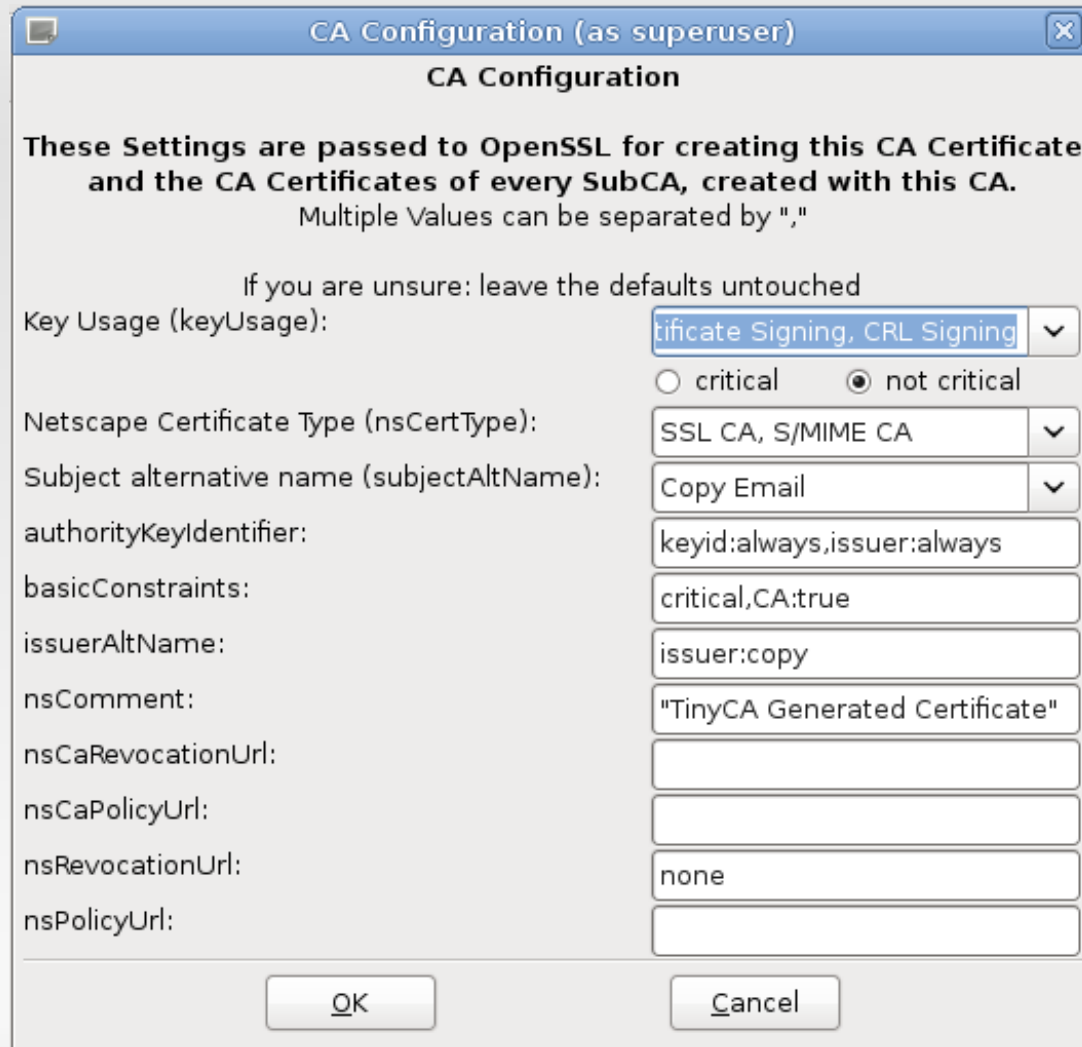
Valid for (Days): 3650

Keylength: ☐ 1024 ☐ 2048 ☒ 4096

Digest: ☒ SHA-1 ☐ MD2 ☐ MDC2 ☐ MD4 ☐ MD5 ☐ RIPEMD-160

OK Cancel

Create certificate



CA Configuration (as superuser)

CA Configuration

These Settings are passed to OpenSSL for creating this CA Certificate and the CA Certificates of every SubCA, created with this CA.
Multiple Values can be separated by ","

If you are unsure: leave the defaults untouched

Key Usage (keyUsage): Certificate Signing, CRL Signing ▼
☐ critical ☒ not critical

Netscape Certificate Type (nsCertType): SSL CA, S/MIME CA ▼

Subject alternative name (subjectAltName): Copy Email ▼

authorityKeyIdentifier: keyid:always,issuer:always

basicConstraints: critical,CA:true

issuerAltName: issuer:copy

nsComment: "TinyCA Generated Certificate"

nsCaRevocationUrl:

nsCaPolicyUrl:

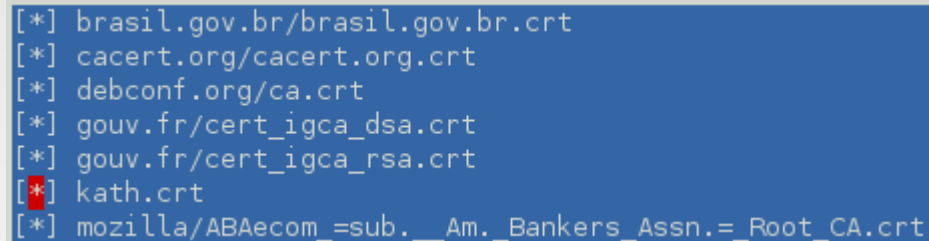
nsRevocationUrl: none

nsPolicyUrl:

OK Cancel

Create certificate

- Copy cacert.pem into /usr/share/ca-certificates/kath.crt
- Make it readable: `chmod 755 /usr/share/ca-certificates/kath.crt`
- `dpkg-reconfigure ca-certificates`
 - Trust new certificates → yes
 - Tick kath.crt
- Symlink in webspace for certificate:
 - `ln -s /usr/share/ca-certificates/kath.crt /var/www/kath.crt`



```
[*] brasil.gov.br/brasil.gov.br.crt
[*] cacert.org/cacert.org.crt
[*] debconf.org/ca.crt
[*] gouv.fr/cert_igca_dsa.crt
[*] gouv.fr/cert_igca_rsa.crt
[*] kath.crt
[*] mozilla/ABAAecom_sub_._Am._Bankers_Assn._Root_CA.crt
```

Certificate settings

- Go to Preferences → openSSL configuration → Server Certificate Settings

Subject alternative name (subjectAltName): ▼

☐ IP Address ☐ DNS Name ☒ raw

- Create certificate:



Create certificate

Create a new Certificate Request

Common Name (eg. your Name, your eMail Address or the Servers Name)	kath-server
eMail Address:	k.hembach@mytum.de
Password (protect your private Key):	●●●●●●●●●●
Password (confirmation):	●●●●●●●●●●
Country Name (2 letter code):	DE
State or Province Name:	Bayern
Locality Name (eg. city):	Munich
Organization Name (eg. company):	TUM
Organizational Unit Name (eg. section):	Biolab
Keylength:	<input checked="" type="radio"/> 4096 <input type="radio"/> 1024 <input type="radio"/> 2048
Digest:	<input checked="" type="radio"/> SHA-1 <input type="radio"/> MD2 <input type="radio"/> MDC2 <input type="radio"/> MD4 <input type="radio"/> MD5 <input type="radio"/> RIPEMD-160
Algorithm:	<input checked="" type="radio"/> RSA <input type="radio"/> DSA

Create certificate & export



Sign Request (as superuser)

Sign Request/Create Certificate

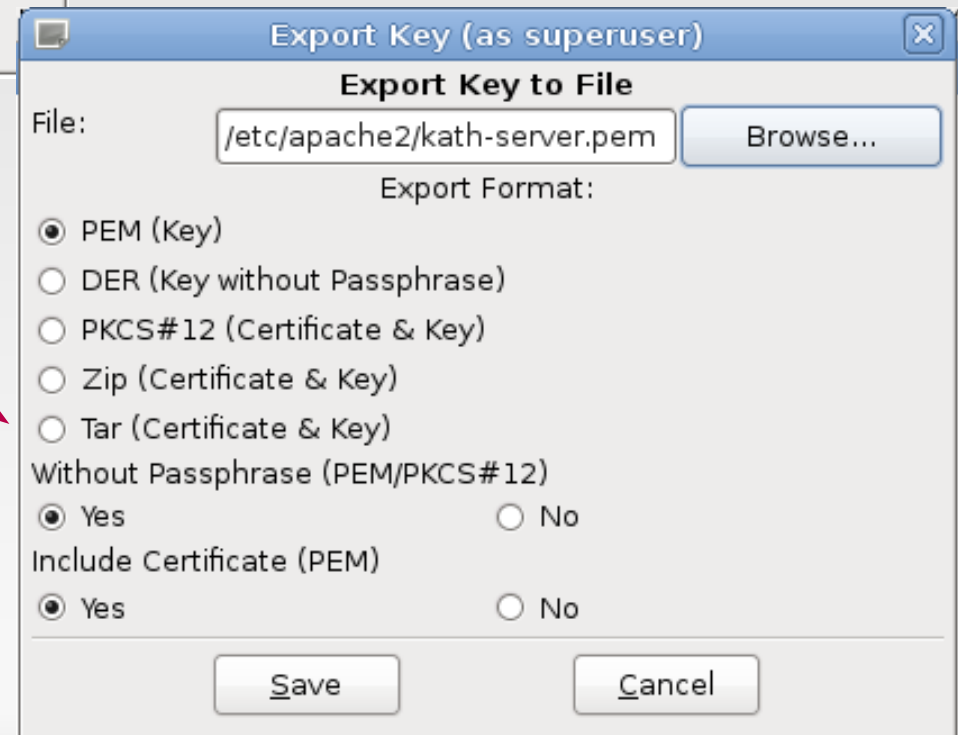
CA Password: [password field]

Valid for (Days): [365]

Subject alternative name (raw): [IP:192.168.16.6,DNS:kath.tbl]

Add eMail Address to Subject DN: ☐ Yes ☒ No

[OK] [Cancel]



Export Key (as superuser)

Export Key to File

File: [/etc/apache2/kath-server.pem] [Browse...]

Export Format:

- ☒ PEM (Key)
- ☐ DER (Key without Passphrase)
- ☐ PKCS#12 (Certificate & Key)
- ☐ Zip (Certificate & Key)
- ☐ Tar (Certificate & Key)

Without Passphrase (PEM/PKCS#12)

- ☒ Yes ☐ No

Include Certificate (PEM)

- ☒ Yes ☐ No

[Save] [Cancel]

- make file only readable by root:
chmod 700 /etc/apache2/kath-server.pem

Enable SSL

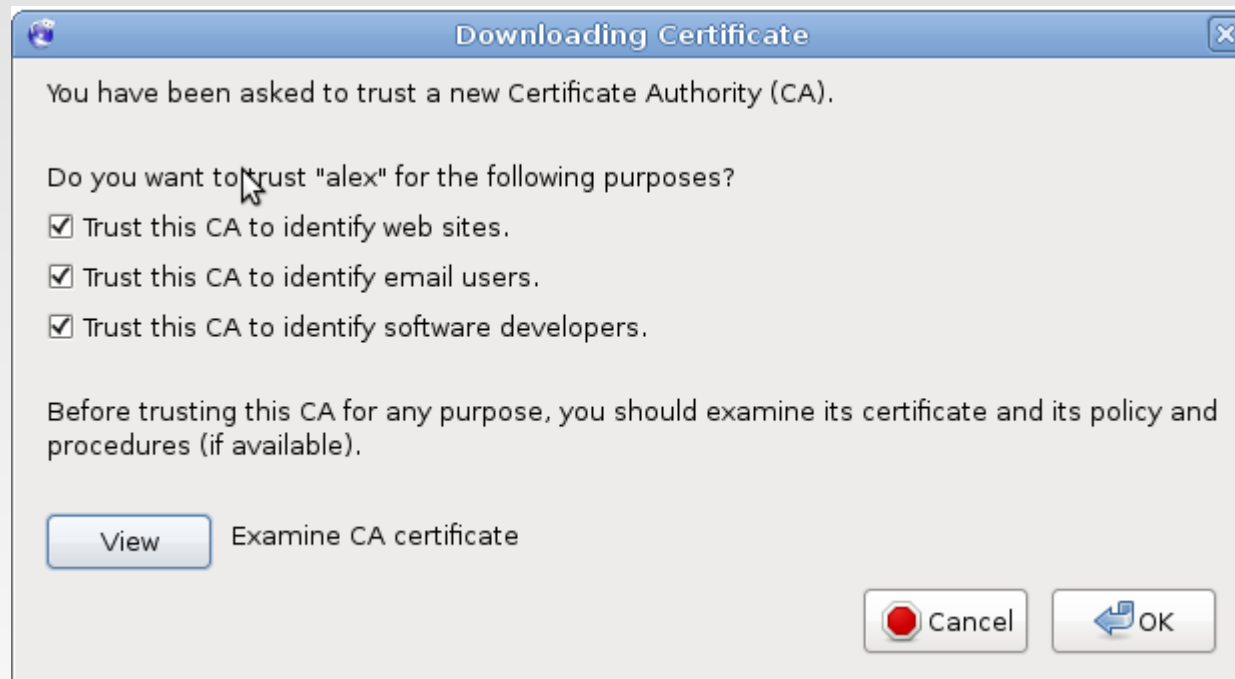
- Edit `/etc/apache2/sites-available/default-ssl:`
 - Set: `SSLCertificateFile /etc/apache2/kath-server.pem`
 - comment “`SSLCertificateKeyFile`” out

```
# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
SSLCertificateFile    /etc/apache2/kath-server.pem
#SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
```

- Enable apache site: **a2ensite default-ssl**
- Enable module ssl: **a2enmod ssl**
- Restart apache to activate changes: **service apache2 restart**

Test certificate

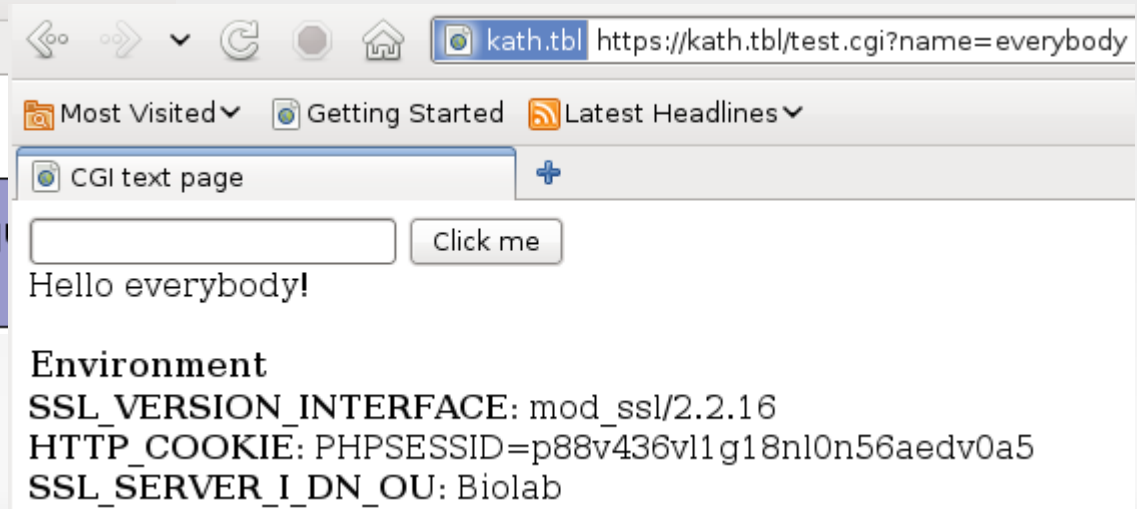
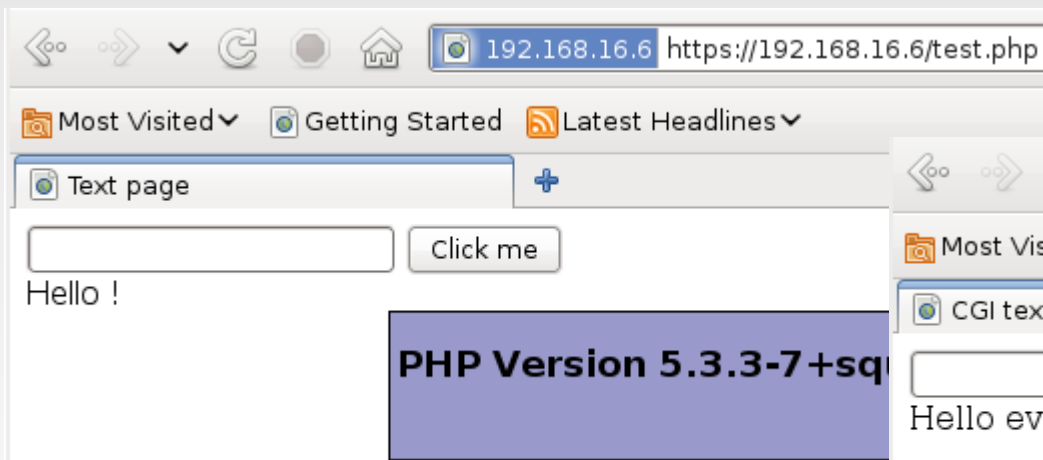
- go to <http://kath.tbl/kath.crt>
- import and trust certificate



- Test if it works: go to <https://kath.tbl/test.cgi> (/test.php)

Activate CGI

- CGI does not work → enable CGI in configuration file `/etc/apache2/sites-available/default-ssl`
 - Options `+ExecCGI`
 - AddHandler `cgi-script cgi py`



Overview

- set up apache
- php and CGI web pages
- phpldapadmin & LAM
- per-user web-accessible directories
- set up https
- create secure section

Create secure section

- secure section of the website that requires authentication and is only accessible via https
- Create directory `/var/www/secure`
- Create `.htaccess`:

```
SSLRequireSSL
AuthName "You shall not pass"
AuthType Basic
AuthBasicProvider ldap
AuthzLDAPAuthoritative on
AuthLDAPURL ldap:///ou=people,dc=tbl?uid
AuthLDAPGroupAttribute memberUid
require valid-user
```

Do not ignore .htaccess files

- Edit /etc/apache2/sites-available/default-ssl
 - Set AllowOverride All

```
<Directory /var/www/>  
    Options Indexes FollowSymLinks MultiViews  
    Options +ExecCGI  
    AddHandler cgi-script cgi py  
    AllowOverride All  
    Order allow,deny  
    allow from all  
</Directory>
```

Enable Idap authentication

- `a2enmod authnz_ldap`
- `service apache2 restart`
- Test `https://kath.tbl/secure/index.html` (and try also http)

